REMARKS

In the Office Action identified above, the Examiner rejected claims 1-9, 12-16, 18-20, 23-31, 34-42, and 45-48 under 35 U.S.C. 102(e) as anticipated by Johnson et al. (U.S. Patent No. 5, 870, 470); rejected claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 under 35 U.S.C. 103(a) as unpatentable over Johnson et al., in view of Adams et al. (U.S. Patent No. 6,031,911). Based on the reasoning set forth below, Applicants respectfully traverse the Examiner's rejections under 35 U.S.C. § 102 and § 103(a).

I. The Rejection of Claims 1-9, 12-16, 18-20, 23-31, 34-42, and 45-48 Under 35 U.S.C. § 102

Claims 1-9, 12-16, 18-20, 23-31, 34-42, and 45-48 were rejected under 35 U.S.C. § 102(e) as being anticipated by Johnson et al. Applicants respectfully traverse this rejection.

In order to support a rejection under 35 U.S.C. § 102(e), each and every element as set forth in the claims must be found, either expressly or inherently described, in a single prior art reference. M.P.E.P. § 2131. Johnson et al. fails to teach each and every recitation of claims 1-9, 12-16, 18-20, 23-31, 33-42, and 45-48.

Claim 1 recites "[a]n encryption apparatus for converting a plaintext block depending on supplied key information," including *inter alia*, "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus." Johnson et al. teaches a masking procedure that "calculates a first mask value 208 (mask 1) on part B (204) using a first generator function (G1) 206" and that "mask 1 (208) is then combined (210) with part A (202) to produce an intermediate-stage part A (212)." *See* Johnson et al., col. 4, line

64-col. 5, line 2. Further, Johnson et al. teaches that "[t]he combining operation 210 may be an Exclusive-OR operation." *See* Johnson et al., col. 5, lines 2-3. Additionally, Johnson et al. teaches that "a second mask value 216 (mask 2) is calculated on intermediate-stage part A (212) using a second generator function 214 (G2)" and that "[m]ask 2 is Exclusive-Ored (218) with part B (204) to produce masked part B (220)." However, Johnson et al. does not teach or suggest at least the step of "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus," as recited in claim 1.

The Examiner alleges that "the prior art (Johnson) does show in Figure 2, the influence of the first mask (the mask used on the plaintext bits of part B) is removed through the computations with plaintext part A and the use of a one-way generator function that produces a second mask which is then XOR with plaintext part B to form the ciphertext (masked Part B). When the second XOR (218) is applied, the influence of the first is removed." However, in Johnson et al., the masked key block is formed from intermediate part A (i.e., influenced by mask 1) Exclusive –ORed with a third mask (which is influenced by mask 2). *See* Johnson et al., col. 5, lines 7-16. Therefore, Johnson et al. fails to teach or suggest at least the step of "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus," as recited in claim 1. Furthermore, in FIG. 2 of Johnson et al., the exclusive OR by XOR 210 is that of PART A and MASK 1 and the exclusive OR by XOR 218 is that of PART B and MASK 2. Since MASK1 and PARTB are different values, the influence of the mask caused by XOR 210 cannot be eliminated by XOR 218. Applicants respectfully request the Examiner to reconsider and

withdraw the rejection of claim 1 under 35 U.S.C. § 102(e) as being anticipated by Johnson et al.

Claims 2, 3, 12, 13, 14, 23, 24, 25, 34, 35, 36, 45, and 46, although of different scope, recite elements similar to that discussed above with regard to claim 1. Applicants therefore request the Examiner to withdraw the rejection of claims 2, 3, 12, 13, 14, 23, 24, 25, 34, 35, 36, 45, and 46 for at least the same reasons discussed above with respect to claim 1.

Claims 4-9, 15-16, 18-20, 26-31, 37-42, and 45-48 depend from claims 1-3, 12-14, 23-25, and 34-36. As explained, claims 1-3, 12-14, 23-25, and 34-36 recite elements not disclosed by Johnson et al. Accordingly, claims 4-9, 15-16, 18-20, 26-31, 37-42 are allowable over Johnson et al. for at least the same reasons as claims 1-3, 12-14, 23-25, and 34-36. Applicants therefore respectfully request that the rejection of these claims under 35 U.S.C. § 102(e) be withdrawn and the claims allowed.

II The Rejection of Claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 Under 35 U.S.C. § 103

Applicants respectfully traverse the rejection of claims 10, 11, 21, 22, 32, 33, 43, 44, 49, and 50 under 35 U.S.C. § 103(a) as unpatentable over Johnson et al. and Adams et al. because the Examiner has failed to establish a *prima facie* case of obviousness.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, the prior art reference (or references when combined) must teach or suggest all the claim elements. Furthermore, "[a]ll words in a claim must be considered in judging

the patentability of that claim against the prior art." *See* M.P.E.P. § 2143.01 (8th Ed., Aug. 2001), quoting *In re Wilson*, 424 F.2d 1382, 1385, 165 U.S.P.Q. 494, 496 (C.C.P.A. 1970). Second, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings. Finally, there must be a reasonable expectation of success. *See* M.P.E.P. § 2143 (8th Ed. 2001), pp. 2100-122 to 127.

Claim 10-11, 21-22, 32-33, 43-44, and 49 depend from claims 1, 12, 23, 34, and 46, respectively, and thus require all the elements of claims 1, 12, 23, 34, and 46. As explained above, Johnson et al. fails to teach or suggest at least the step of "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus," as recited in claim 1.

Adams et al. does not make up for the deficiencies of Johnson et al. That is, Adams et al. also fails to teach or suggest at least "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus," as recited in claim 1. Indeed, the Examiner merely used Adams et al. to show the use of Hamming weights but makes no attempt to show where the reference teaches the step of "means for removing an influence of the selected mask patterns from the ciphertext block before the ciphertext block is output from said encryption apparatus," as recited in claim 1.

Since the cited references fail to teach each and every element required by claims 10-11, 21-22, 32-33, 43-44, and 49, no prima facie case of obviousness has been made out with respect to these claims. Applicants respectfully request the

Examiner to reconsider and withdraw the rejection of claims 10-11, 21-22, 32-33, 43-44, and 49 under 35 U.S.C. § 103 as being obvious from Johnson et al. in view of Adams et al.

III. Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to our deposit account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: December 27, 2004

By: _____
Milan Kapadia
Reg. No. 55,982